USE OF INTERNET WEB TECHNOLOGY FOR WIRELESS INTERNET ACCESS

This is a continuation-in-part of application Serial No. 09/626,699, filed July 27, 2000, entitled “USE OF INTERNET WEB TECHNOLOGY TO REGISTER WIRELESS ACCESS CUSTOMERS” which is a continuation- in- part Serial No. 09/432,824, filed November 2, 1999, entitled, ‘CELLULAR WIRELESS INTERNET ACCESS SYSTEM USING SPREAD SPECTRUM AND INTERNET PROTOCOL (IP).”

INTRODUCTION

The present invention is directed to the use of Internet web technology for wireless customer Internet access AND specifically to allow authenticated Internet access for more than one personal computer.

BACKGROUND OF THE INVENTION

Both of the above applications describe a cellular wireless Internet access system which operates in the 2 gigahertz or other frequency bands to provide high data rates to fixed and portable wireless Internet devices. Such users connect to near-by base stations which in turn communicate to Integrated Network Controllers which are then connected to the Internet. Such wireless implementation relates to an access network of the UMTS

A-68747/JGW
November 14, 2000
1029728

(Universal Mobile Telephone Service) and its subset UTRAN (Universal Terrestrial Radio Access Network) standards.

In order to gain service in a cellular wireless network of the types similar to the above, a sales representative at a retail location typically takes customer information, credit card number and credit history, etc. That information is used to create an account with a cellular service provider, with the customer information stored on the service provider's Home Location Register (HLR) or other customer database. A SIM (Subscriber Identity Module) card is then associated with the account and placed within the cellular terminal (typically, a mobile phone or wireless Internet device).

Both of the above techniques are cumbersome, requiring action on the part of the retailer or network service provider, and creating a time delay before a new customer can use the service.

Application Serial No. 09/626,699, allows the user to self-register to gain access to Internet services for the wireless system as above. It is, however, also desired to allow authenticated access to be provided for various user access units.

OBJECT AND SUMMARY OF INVENTION

It is therefore an object of the present invention to provide an improved method for allowing customer access in a wireless Internet system.

In accordance with the above object there is provided a method of operating a cellular wireless Internet access system as part of an Internet Network where users have personal computers (PCs) and each user utilizes a portable user equipment (UE) typically with a directly attached antenna for communicating in a wireless manner on a cellular network with an integrated network controller, the UE being connected to the PC, the network

having a registration web server and an access operator authentication server. The method comprises the following steps:

A PC and associated UE are used to register with a registration web server on the Internet Network via an anonymous connection to the network including downloading subscriber identity information from the registration web server to the PC via the UE for storage in the PC. The subscriber identity information includes, at least, a unique user identification (user ID) and a permanent password. Such stored information constitutes a virtual subscriber identity module (VSIM). The access operator authentication server is updated with the user ID and password. The user may then be connected to an allowable Internet service provider (ISP) using the VSIM. Another PC may be used by transferring electronically the user ID and password to the other PC, said transfer including one of the following; temporary transfer to portable magnetic storage means, a local area network (LAN) or e-mail attachments, or similar electronic transfer.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram of an Internet system illustrating the present invention.

FIG. 2 is a schematic block diagram illustrating the present invention.

FIG. 3 is a flowchart showing the operation of the invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENT

Referring now to FIG. 1, there is illustrated a wireless access user 22 with user equipment (UE) connected by typical data connection to the personal computer (PC). The personal computer has a CD drive or similar media input device with a special compact disc containing software, including a wizard (that is the instructional system procedures for registration) which is placed in the CD drive. In addition, a second PC and UE 21 is

illustrated designated, new PC whose function in the Internet Network system shown in FIG. 1 will be described below.

Both the UE and CD of system 22 are acquired and purchased at some retail location or by mail. This is described more fully in the above '699 application involving registration. PC 22 and its associated UE as described in the above application Serial No. 09/432,824, are a part of a UMTS/UTRAN system which by many wireless techniques (a specific novel one is described in the above application) communicates in a wireless manner via a UTRAN network as indicated by the symbol 23 to an Integrated Network Controller (INC) 24. Such controller may be connected by wireline or otherwise to an Internet Protocol (IP) Network 31. As discussed in the above pending application, the Integrated Network Controller 24 includes an RNC or Radio Network Controller 26 which controls and allocates the radio network resources and provides reliable delivery of user traffic between a base station (described in the above pending application) and User Equipment (UE) and eventually the Integrated Network Controller (INC) 24. An SGSN (Serving General Packet Radio Service Support Node) 27 provides session control and connection to the Access Operator Radius Authentication Server 34. Lastly, LAC 28 (layer 2 Tunneling Protocol Access Concentrator) provides the gateway functionality to the allowable Internet Service Providers (ISP) 40 and to the registration server 36. A Layer 2 Tunneling Protocol Network Server (LNS) 30 terminates communication tunnels from the LAC through the IP network. The Access Operator Radius Authentication Server 34 supports the Home Location Register (HLR) functionality (described in the above pending application). The Access Operator Registration Server 36 provides the facilities for a new user to register.

The Integrated Network Controller 24 also illustrates that it incorporates a "RADIUS" client 29. RADIUS is a system including the software that supports centralized access control for Internet access, which, as discussed above, is traditionally used where the access to the Internet is via the public switched telephone network. A description of

RADIUS is provided by an article RFC 2138 Remote Authentication Dial-in User Service (RADIUS) by C. Rigney, et al., April 1997.

In all cases of communication of a user equipment 21 or 22 through the Internet Protocol Network, illustrated as 31, authentication is performed by the user equipment (UE) signaling the customer's wireless access authentication information which is passed over the air to Integrated Network Controller 24 which queries a RADIUS server authentication server with the user ID (identification) and temporary password. The RADIUS server used is the Access Operator's RADIUS Authentication Server 34 which communicates with the Integrated Network Controller via the IP network using UDP/IP protocols with additional protocol layers for security.

In the case of a new user, a 'new user' ID and temporary password, preprogrammed in the CD software, is signaled to the Access Operator RADIUS Authentication Server 34 via the INC 24. The Access Operator RADIUS Authentication Server 34 recognizes the user as a 'new user' and communicates a set of protocol filters to the INC 24 that results in a PPP (Point-to-Point Protocol) session being set up between the User's PC and the Access Operator's Registration Server 36 via the Layer 2 Tunneling Protocol communication link 32 and bars the user from accessing any other service. The Access Operator's Registration Server 36 is connected to the subscriber account management and billing system 37.

Thus, the foregoing constitutes the anonymous session link where a general or non-authenticated user can still gain access to the wireless access operator's registration server for the purpose of new-user registration. The accompanying legend indicates the various paths. A UMTS access network operator 33 provides the special servers 34 and 36 along with the billing system 37.

The flow chart of FIG. 3 describes in somewhat truncated detail the registration procedure set out in greater detail in the above co-pending '699 application. After "START" in Step

1, the user purchases the user equipment UE which may or may not have a particular unique identification number (ID) and a CD with the appropriate software and wizard feature installed on it. This is connected to the PC. Next in Step 2, the user equipment is installed on the PC via the wizard instructions on the CD, along with a new user ID and temporary password which were contained on the CD. These are then sent to the UE. The UE sends this authentication information over the air to the RNC 26, which is passed onto the RADIUS Client 29 and the SGSN 27 which queries the RADIUS server 34 with a new user ID and temporary new user password. In effect, an anonymous connection using the temporary password is made on the Internet and as described in the above co-pending application, a permanent password is generated along with a user ID. As indicated in Step 3, this is stored in the PC memory of the unit 22. Thus, the permanent password and ID which have been electronically stored in the PC memory (which may be a randomly accessible memory or floppy disk or hard disk) form a virtual subscriber identity module or VSIM. At the same time (Step 6), the RADIUS server 34 is updated with the user's name and permanent password to provide subsequent access to allowable ISPs 40, as illustrated in FIG. 1. Thus, as described in the above co-pending application, access has been gained to the Internet Network on a special anonymous connection. Thus, as described in Step 4, connection may now be made to allowable Internet service providers (ISPs) using the VSIM user information via the Layer 2 Tunneling Network Server (LNS) 45 of the allowable ISPs 40. This route is shown in a dashed line designated End User Traffic 46.

With the VSIM, in accordance with the present invention, as shown in Step 6, a user may electronically transfer the subscriber identity information to a new or another PC, for example, indicated as 21 in FIG. This is illustrated in FIG. 2 where the original PC 22 with the VSIM subscriber identity module information indicated in dashed outline transfers the VSIM information via one of the following electronic techniques so designated: floppy disk, LAN (Local Area Network), e-mail attachment or other electronic means. Thus, the new PC 21 contains the VSIM information so designated in the dashed block as VISIM′and may access the Internet Network. Optionally, if as part of the VSIM or subscriber identity information, the unique identification or ID of the original associated

UE with PC 22 is part of the VSIM information, then as shown by the optional line 47 the original or old UE must be transferred to the new PC 21. This prevents use by more than one subscriber; in other words, it is further protection against fraud. However, this is not necessary if the user equipment ID is not a part of the required VSIM information.

Thus, with the foregoing the new PC 21 may now access the Internet Network. In summary the VSIM may manifest itself as the file on the hard disk of the personal computer being used for Internet Access, or as an alternative, be stored on a floppy disk or other removable media. In the case of the VSIM being stored on a floppy disk the end user may take that disk to a new or different computer connected to a new or different UE and gain wireless access to the Internet. Moreover, if the VSIM information is not encrypted, it can be retrieved and manually recorded by the user for transfer to another computer.

Authentication and accounting is provided for against the identifying information of their VSIM. Other typical functions of a subscriber identity module (SIM) may be provided in addition to the unique ID, a customer password, and UE equipment identifier. This may include storage of an access network operator name, an Internet service provider name, encryption of all of the above data, provision of all of the above data on demand to associated subscriber equipment to an access network operator, or on demand to an ISP.

In conclusion, with the use of the VSIM as described above in a mobile or portable wireless system, such information is transportable in this electronic format from one computer to another. Moreover, it is stored in the user's PC or personal computer rather than the separate user equipment or subscriber unit (such as a cellular telephone).